Multi-Factor Authentication

We take your online security seriously. Therefore, we have implemented Multi-Factor Authentication for our online CU@Home access.

What Is It?
Multi-Factor Authentication is a tool that provides extra protection for your online data and helps guard against fraudulent online activities like phishing scams (malicious requests for personal information) and identity theft.

How Does It Work?
In addition to your User ID and Password, the system will ask you to select three security questions, one image, and one pass phrase. The system will require the User ID and the correct combination of the image and pass phrase before allowing you to complete the log in process.

How Does It Protect Me Against Phishing?
When logging into CU@Home, the system associates your username with the image and pass phrase you selected. This protects your accounts from fraudulent access and also reassures you that you have not accessed a spoof of our website.

Helpful Hints for Answering Security Questions.
With the development of social media and people's willingness to "tell it all". We have become easy target for con artists. We've found that scammers are able to gather enough information from social media websites to answer the standard security questions. So, we've developed helpful hints for you to be able to answer your questions, without using the true answers to those questions.

- ***Use the same answer for each question***. In this instance, you would choose one word to represent the answer to each of your questions.
- ***Choose the opposite answer for each question***. So, if asked what is your mother's middle name, your answer would be your father's middle name.
- ***Apply the questions to your spouse***. In this instance, if you and your spouse attended to different schools and your question was "what high school did you attend", your answer would be that of your spouse.